2025 Provide Updated ISACA CISM Dumps as Practice Test and PDF [Q324-Q341

2025 Provide Updated ISACA CISM Dumps as Practice Test and PDF
CISM Dumps are Available for Instant Access

To be eligible to take the CISM exam, candidates must have a minimum of five years of experience in information security, with at least three years in information security management. Alternatively, candidates can substitute a maximum of two years of general work experience for a year of information security experience. Candidates must also adhere to ISACA's Code of Professional Ethics.

ISACA CISM (Certified Information Security Manager) certification is a globally recognized credential for information security professionals who manage, design, and oversee an organization's information security program. Certified Information Security Manager certification demonstrates expertise in developing and implementing information security strategies and policies that align with business objectives. The CISM certification is ideal for IT professionals looking to advance their careers in the field of information security management.

Q324. Which of the following is an example of a corrective control?

* Diverting incoming traffic upon responding to the denial of service (DoS) attack
* Filtering network traffic before entering an internal network from outside
* Examining inbound network traffic for viruses
* Logging inbound network traffic

Section: INCIDENT MANAGEMENT AND RESPONSE

Explanation

Explanation:

Diverting incoming traffic corrects the situation and, therefore, is a corrective control. Choice B is a preventive control. Choices C and D are detective controls.

Q325. Which of the following has the GREATEST impact on efforts to improve an organization’s security posture?

* Regular reporting to senior management
* Supportive tone at the top regarding security
* Automation of security controls
* Well-documented security policies and procedures

Explanation

The supportive tone at the top regarding security is the greatest impact on efforts to improve an organization’s security posture. This means that senior management should demonstrate their commitment and leadership to information security by setting clear goals, allocating adequate resources, communicating effectively, and rewarding good practices. A supportive tone at the top can also influence the culture and behavior of the organization, as well as foster trust and collaboration among stakeholders12. References = CISM Review Manual 15th Edition, page 1261; CISM Item Development Guide, page 82

Q326. An information security team is planning a security assessment of an existing vendor. Which of the following approaches is MOST helpful for properly scoping the assessment?

* Review the vendor’s security policy.
* Review controls listed in the vendor contract.
* Focus the review on the infrastructure with the highest risk.
* Determine whether the vendor follows the selected security framework rules.

Q327. Which of the following is the PRIMARY purpose of establishing an information security governance framework?

* To minimize security risks
* To proactively address security objectives
* To reduce security audit issues
* To enhance business continuity planning

Q328. To address the issue that performance pressures on IT may conflict with information security controls, it is MOST important that:

* noncompliance issues are reported to senior management
* information security management understands business performance issues
* the security policy is changed to accommodate IT performance pressure
* senior management provides guidance and dispute resolution

Section: INFORMATION SECURITY PROGRAM MANAGEMENT

Q329. Which is the MOST important driver for effectively communicating the progress of a new information security program’s implementation to key stakeholders?

* facilitating stakeholder undemanding of program-related technology concepts

* Designing universal key performance indicators (KPIs) for the program
* Understanding stakeholder needs that influence program objectives
* Documenting risk that could impact achievement of program objectives

32:35

Q330. Which of the following is MOST critical for the successful implementation and maintenance of a security policy?
* Assimilation of the framework and intent of a written security policy by all appropriate parties
* Management support and approval for the implementation and maintenance of a security policy
* Enforcement of security rules by providing punitive actions for any violation of security rules
* Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Section: INCIDENT MANAGEMENT AND RESPONSE

Explanation

Explanation:

Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules, is also required, along with the user’s education on the importance of security.

Q331. What would be an information security manager’s BEST recommendation upon learning that an existing contract with a third party does not clearly identify requirements for safeguarding the organization’s critical data?
* Cancel the outsourcing contract.
* Transfer the risk to the provider.
* Create an addendum to the existing contract.
* Initiate an external audit of the provider’s data center.

The Definition of an addendum is an item of additional material added at the end of a book or document, typically in order to correct, clarify, or supplement something.

Q332. An information security team is planning a security assessment of an existing vendor. Which of the following approaches is MOST helpful for properly scoping the assessment?
* Focus the review on the infrastructure with the highest risk
* Review controls listed in the vendor contract
* Determine whether the vendor follows the selected security framework rules
* Review the vendor’s security policy

Reviewing controls listed in the vendor contract is the most helpful approach for properly scoping the security assessment of an existing vendor because it helps to determine the security requirements and expectations that the vendor has agreed to meet. A vendor contract is a legal document that defines the terms and conditions of the business relationship between the organization and the vendor, including the scope, deliverables, responsibilities, and obligations of both parties. A vendor contract should also specify the security controls that the vendor must implement and maintain to protect the organization’s data and systems, such as encryption, authentication, access control, backup, monitoring, auditing, etc. Reviewing controls listed in the vendor contract helps to ensure that the security assessment covers all the relevant aspects of the vendor’s security posture, as well as to identify any gaps or discrepancies between the contract and the actual practices.

Therefore, reviewing controls listed in the vendor contract is the correct answer.

References:

* https://medstack.co/blog/vendor-security-assessments-understanding-the-basics/

* https://www.ncsc.gov.uk/files/NCSC-Vendor-Security-Assessment.pdf

* https://securityscorecard.com/blog/how-to-conduct-vendor-security-assessment

Q333. An intrusion has been detected and contained. Which of the following steps represents the BEST practice for ensuring the integrity of the recovered system?
* Install the OS, patches, and application from the original source.
* Restore the OS, patches, and application from a backup.
* Restore the application and data from a forensic copy.
* Remove all signs of the intrusion from the OS and application.

After an intrusion has been detected and contained, the system should be recovered to a known and trusted state. The best practice for ensuring the integrity of the recovered system is to install the OS, patches, and application from the original source, such as the vendor’s website or media. This way, any malicious code or backdoors that may have been inserted by the intruder can be eliminated. Restoring the OS, patches, and application from a backup may not guarantee the integrity of the system, as the backup may have been compromised or outdated. Restoring the application and data from a forensic copy may preserve the evidence of the intrusion, but it may also reintroduce the vulnerability or malware that allowed the intrusion in the first place. Removing all signs of the intrusion from the OS and application may not be sufficient or feasible, as the intruder may have made subtle or hidden changes that are difficult to detect or undo.

References =

* ISACA, CISM Review Manual, 16th Edition, 2020, page 2401

* ISACA, CISM Review Questions, Answers & Explanations Database – 12 Month Subscription, 2020, question ID 2132
The BEST practice for ensuring the integrity of the recovered system after an intrusion is to restore the OS, patches, and application from a backup. This will ensure that the system is in a known good state, without any potential residual malicious code or changes from the intrusion. Restoring from a backup also enables the organization to revert to a previous configuration that has been tested and known to be secure. This step should be taken prior to conducting a thorough investigation and forensic analysis to determine the cause and extent of the intrusion.

Q334. Which of the following is MOST appropriate to add to a dashboard for the purpose of illustrating an organization’s risk level to senior management?
* Risk heat map
* Results of risk and control testing
* Budget variance for information security

Q335. When collecting admissible evidence, which of the following is the MOST important requirement?
* Need to know
* Preserving audit logs
* Due diligence
* Chain of custody

Explanation

Chain of custody is the MOST important requirement when collecting admissible evidence, because it ensures the integrity and authenticity of the evidence by documenting its history, handling, and storage. Chain of custody records who, what, when, where, why, and how the evidence was collected, analyzed, and preserved.

Without a proper chain of custody, the evidence may be challenged or rejected in a court of law. Need to know, preserving audit logs, and due diligence are important aspects of evidence collection, but they are not as critical as chain of custody. References = CISM Review Manual, 16th Edition, page 3031; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1492The most important requirement when collecting admissible evidence is the chain of custody. The chain of custody is a documented record of who had control of the evidence at any given time, from the point of collection until the evidence is presented in court. This is important in order to ensure the evidence can be authenticated and is not subject to tampering or any other form of interference. Other important considerations include need to know, preserving audit logs, and due diligence.

Q336. What should be an information security manager’s MOST important consideration when developing a multi- year plan?
* Ensuring contingency plans are in place for potential information security risks
* Ensuring alignment with the plans of other business units
* Allowing the information security program to expand its capabilities
* Demonstrating projected budget increases year after year
= The most important consideration when developing a multi-year plan for information security is to ensure alignment with the plans of other business units. Alignment means that the information security plan supports and enables the achievement of the business objectives, strategies, and priorities of the organization and its various units. Alignment also means that the information security plan is consistent and compatible with the plans of other business units, and that it addresses the needs, expectations, and requirements of the relevant stakeholders1 .

By ensuring alignment with the plans of other business units, the information security manager can achieve the following benefits1 :

* Increase the value and effectiveness of information security: By aligning the information security plan with the business goals and drivers, the information security manager can demonstrate the value and contribution of information security to the organization’s performance, growth, and competitiveness.

The information security manager can also ensure that the information security plan addresses the most critical and relevant risks and opportunities for the organization and its units, and that it provides adequate and appropriate protection and support for the organization’s assets, processes, and activities.

* Enhance the communication and collaboration with other business units: By aligning the information security plan with the plans of other business units, the information security manager can enhance the communication and collaboration with the other business unit leaders and managers, who are the key stakeholders and partners in information security. The information security manager can also solicit and incorporate their input, feedback, and suggestions into the information security plan, and provide them with timely and relevant information, guidance, and support. The information security manager can also foster a culture of trust, respect, and cooperation among the different business units, and promote a shared vision and commitment to information security.

* Optimize the use and allocation of resources for information security: By aligning the information security plan with the plans of other business units, the information security manager can optimize the use and allocation of resources for information security, such as budget, staff, time, or technology. The information security manager can also avoid duplication, conflict, or waste of resources among the different business units, and ensure that the information security plan is feasible, realistic, and sustainable. The information security manager can also leverage the resources and capabilities of other business units to enhance the information security plan, and provide them with the necessary resources and capabilities to implement and maintain the information security plan.

The other options are not the most important consideration when developing a multi-year plan for information security, as they are less strategic, comprehensive, or impactful than ensuring alignment with the plans of other business units. Ensuring contingency plans are in place for potential information security risks is an important component of the information security plan, but it is not the most important consideration, as it focuses on the reactive and preventive aspects of information security, rather than the proactive

and enabling aspects. Allowing the information security program to expand its capabilities is an important objective of the information security plan, but it is not the most important consideration, as it depends on the availability and suitability of the resources, technologies, and opportunities for information security, and it may not align with the organization’s needs, priorities, or constraints. Demonstrating projected budget increases year after year is an important outcome of the information security plan, but it is not the most important consideration, as it reflects the cost and demand of information security, rather than the value and benefit of information security, and it may not be justified or supported by the organization’s financial situation or expectations1 . References = CISM Domain 1: Information Security Governance (ISG) [2022 update], CISM Domain 2: Information Risk Management (IRM) [2022 update], Aligning Information Security with Business Strategy – ISACA, [Aligning Information Security with Business Objectives – ISACA]

Q337. The PRIMARY advantage of a network intrusion detection system (IDS) is that it can:
* detect network vulnerabilities
* simulate denial-of-service attacks.
* block undesirable network traffic
* identify an attack on the network.

Q338. IT projects have gone over budget with too many security controls being added post-production. Which of the following would MOST help to ensure that relevant controls are applied to a project?
* Involving information security at each stage of project management
* Identifying responsibilities during the project business case analysis
* Creating a data classification framework and providing it to stakeholders
* Providing stakeholders with minimum information security requirements

The best way to ensure that relevant controls are applied to a project is to involve information security at each stage of project management. This will help to identify and address the security risks and requirements of the project from the beginning, and to integrate security controls into the project design, development, testing, and implementation. This will also help to avoid adding unnecessary or ineffective controls post-production, which can increase the project cost and complexity, and reduce the project performance and quality. By involving information security at each stage of project management, the information security manager can ensure that the project delivers the expected security value and aligns with the organization’s security strategy and objectives. References = CISM Review Manual 15th Edition, page 41.

Q339. Conducting a cost-benefit analysis for a security investment is important because it
* supports asset classification.
* quantifies return on security investment
* supports justification for expenditure.
* quantifies residual risk

Q340. Which of the following is MOST important to include in a contract with a critical service provider to help ensure alignment with the organization’s information security program?
* Escalation paths
* Right-to-audit clause
* Termination language
* Key performance indicators (KPIs)

Q341. Which of the following is the MOST important consideration when selecting members for an information security steering committee?
* Cross-functional composition
* Information security expertise
* Tenure in the organization
* Business expertise

Updated CISM Dumps Questions For ISACA Exam: https://www.topexamcollection.com/CISM-vce-collection.html]